Reply to Fahmi and Golshani's comment on "Quantum key distribution in the Holevo limit"

Adán Cabello*
Departamento de Física Aplicada II, Universidad de Sevilla, E-41012 Sevilla, Spain
(Dated: February 2, 2008)

As Fahmi and Golshani correctly point out, a protocol introduced in A. Cabello, Phys. Rev. Lett. **85**, 5635 (2000), to show that a quantum key distribution protocol can have efficiency one (i.e., can achieve the Holevo limit), does indeed not have efficiency one. The corrected protocol, introduced in A. Cabello, Recent. Res. Devel. Physics **2**, 249 (2001), is reproduced here.

PACS numbers: 03.67.Dd, 03.67.Hk, 03.65.Ud

As Fahmi and Golshani correctly point out in the preceding Comment [1], a protocol introduced in [2] to show that a quantum key distribution protocol can have efficiency one (i.e., can achieve the Holevo limit), where efficiency is defined as the number of secret bits per transmitted bit plus qubit, does indeed not have efficiency one. This error was already corrected in [3, 4]. For completeness' sake, the corrected protocol introduced in [3, 4], with efficiency one, is reproduced here.

Suppose that the quantum channel is composed of two qubits (1 and 2) prepared with equal probabilities in one of four orthogonal pure states:

$$|\eta_0\rangle = \frac{1}{\sqrt{3}}\left(|00\rangle + |01\rangle + |10\rangle\right), \tag{1a}$$

$$|\eta_1\rangle = \frac{1}{\sqrt{3}}\left(|00\rangle - |01\rangle + |11\rangle\right), \tag{1b}$$

$$|\eta_2\rangle = \frac{1}{\sqrt{3}}\left(|00\rangle - |10\rangle - |11\rangle\right), \tag{1c}$$

$$|\eta_3\rangle = \frac{1}{\sqrt{3}}\left(|01\rangle - |10\rangle + |11\rangle\right). \tag{1d}$$

Alice sends both qubits to Bob. Eve cannot access qubit 2 while she still holds qubit 1. Each pair of qubits encodes 2 bits of the key (for instance, "00" if the state is $|\eta_0\rangle$, "01" if the state is $|\eta_1\rangle$, "10" if the state is $|\eta_2\rangle$, and "11" if the state is $|\eta_3\rangle$). Since the four states (1a)–(1d) are orthogonal, Bob can unambiguously discriminate between them and identify which is the one sent by Alice.

As can be easily checked, the revised protocol does not only satisfy Mor's requirements to prevent cloning when Eve has a one-by-one access to the qubits (namely, that the reduced states of the first subsystem must be non-orthogonal and non-identical, and the reduced states of the second subsystem must be non-orthogonal [5]) for *any* two states chosen from (1a)–(1d), but is also secure against the double C-NOT eavesdropping strategy proposed by Fahmi and Golshani in [1].

* Electronic address: adan@us.es

[1] A. Fahmi and M. Golshani, preceding Comment, Phys. Rev. Lett. **100**, 018901 (2008).
[2] A. Cabello, Phys. Rev. Lett. **85**, 5635 (2000).
[3] A. Cabello, Recent. Res. Devel. Physics **2**, 249 (2001).
[4] A. Cabello, in *Física Cuántica y Realidad. Quantum Physics and Reality*, edited by C. Mataix and A. Rivadulla (Editorial Complutense, Madrid, 2002), p. 333.
[5] T. Mor, Phys. Rev. Lett. **80**, 3137 (1998).